# UNITED STATES DISTRICT COURT

for the

Western District of Washington

| | | |
|---|---|---|
| In the Matter of the Search of<br>*(Briefly describe the property to be searched or identify the person by name and address)*<br>Sixteen (16) SUBJECT DEVICES, stored at FWS OLE Digital Evidence Recovery and Technical Support Unit, SeaTac, Washington, as further described in Attachment A-1 and A-2, incorporated herein by reference. | ) | Case No. MJ20-485 |

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Sixteen (16) SUBJECT DEVICES, stored at FWS OLE Digital Evidence Recovery and Technical Support Unit, SeaTac, Washington, as further described in Attachment A-1 and A-2, incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B for a list of infromation to be disclosed, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| Title 16, U.S.C. § 554<br>Title 16, U.S.C. § 1538<br>Title 16, U.S.C. §3372(A) | Smuggling goods out of the United States, importing or exporting endangered wildlife species, and importing or exporting wildlife taken in violation of United States, State, or foreign law. |

The application is based on these facts:

See attached Affidavit of FWS Special Agent Curtis Knights

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Curtis Knights

*Applicant's signature*

FWS Special Agent Curtis Knights

*Printed name and title*

The above-named agent provided a sworn statement attesting to the truth of the attached affidavit by telephone.

Date: 7/31/2020

*Judge's signature*

City and state: Seattle, Washington

Brian A. Tsuchida, U.S. MAGISTRATE JUDGE

*Printed name and title*

# AFFIDAVIT

STATE OF WASHINGTON )
) ss
COUNTY OF KING )

I, Curtis Knights, being duly sworn, declare and state as follows:

## INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two (2) electronic devices and forensic mirror images of fourteen (14) electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Fish and Wildlife Service ("FWS") and have been employed as a Special Agent since March 2016. I was previously employed by the FWS, Office of Law Enforcement, as a Wildlife Inspector for five years. I have received specialized training and have experience in the enforcement of federal laws including the Lacey Act and the Endangered Species Act ("ESA"), described in greater detail below. I have also received training in and have had experience identifying potentially federally regulated wildlife through visual inspection. I have participated in numerous federal investigations, either as a case agent or officer or in various support roles, including investigations involving the unlawful killing, transport, export, import, possession and sale of wildlife. I have also received training and participated in the execution of search warrants, including search warrants for premises and electronic devices and digital evidence found therein.

## PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search electronic devices, and



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

forensic mirror images from electronic devices ("SUBJECT DEVICES") that were previously seized pursuant to two search warrants authorized in connection with the investigation described below. Following is a description of the SUBJECT DEVICES, all of which are currently located at 17930 International Blvd., SeaTac, Washington, at the offices of the FWS Digital Evidence Recovery and Technical Support Unit:

a. Electronic devices identified at, and subsequently seized from the residential premises of Eugene Lantsman located at 950 72nd Street, Apt. #2A, Brooklyn, New York 11228 ("the New York Premises"):

| **Item Description** | **FWS Evidence Number** |
|---|---|
| 1. Computer housed in a "Cooler Master" brand housing tower and bearing the bar code RC912KKN11131500811 | ST# 075402 Item 1 |
| 2. 1 Terabyte Western Digital WD10EALX Hard Drive bearing the serial number WCATR9321079 | ST# 075402 Item 2 |

b. Electronic devices identified at, and from which forensic mirror images were seized, from the residential premises of Leonid Lantsman located at 704 Devon Place, Alexandria, VA 22314 ("the Virginia Premises"):

| **Item Description (from which forensic mirror images were taken)** | **FWS Evidence Number** |
|---|---|
| 1. Lenovo ThinkPad T560 laptop computer bearing S/N R9-0MEHEJ containing SanDisk SSD hard drive bearing S/N 164813800597 | ST# 064100 Item 1A |
| 2. 8GB SanDisk SD card bearing S/N B11105716254G | ST# 064100 Item 2A |
| 3. 2GB Vector Media USB flash drive | ST# 064100 Item 3A |
| 4. 32 MB Gateway USB flash drive | ST# 064100 Item 4A |
| 5. 2GB SanDisk Cruzer USB flash drive bearing S/N 07741302A3A1446C | ST# 064100 Item 5A |
| 6. 8GB Kingston USB flash drive bearing S/N 201006010301 | ST# 064100 Item 6A |
| 7. 256 MB USB flash drive bearing S/N 1000026150007 | ST# 064100 Item 7A |



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

| | |
|---|---|
| 8. 16GB PNY USB flash drive bearing S/N AA0000000034 | ST# 064100 Item 8A |
| 9. 4GB USB flash drive | ST# 064100 Item 9A |
| 10. 2GB SanDisk SD card bearing S/N BE0808713287G | ST# 064100 Item 10A |
| 11. 2GB Exelis USB flash drive bearing S/N 9E4F9DAA | ST# 064100 Item 11A |
| 12. 1GB unknown model USB flash drive | ST# 064100 Item 12A |
| 13. 16GB Patriot USB flash drive with S/N 070C4421A506AC63 | ST# 064100 Item 13A |
| 14. 64GB SanDisk Cruzer USB flash drive with S/N 4C530001310607113470 | ST# 064100 Item 18A |

4. The warrant would authorize a search of the SUBJECT DEVICES from the New York Premises and mirror images of the SUBJECT DEVICES found at the Virginia Premises, as well as a forensic examination of their content, for the purpose of identifying electronically stored data as particularly described in Attachment B incorporated by reference, for evidence, fruits, and instrumentalities of violations of: 16 U.S.C. § 554 (smuggling goods out of the United States); 16 U.S.C. § 1538 (importing, exporting, taking, possessing, selling, delivering, receiving and offering for sale in interstate or foreign commerce endangered or threatened species of wildlife); 16 U.S.C. § 3372(a) (importing, exporting, transporting, selling, receiving, acquiring and purchasing in interstate or foreign commerce any fish or wildlife taken, possessed, transported, or sold in violation of any law or regulation of the United States or any State, or in violation of any foreign law); 16 U.S.C. § 3372(d) (making or submitting any false record or label for, or any false identification of, any wildlife which has been, or is intended to be, transported in interstate commerce or foreign commerce); 18 U.S.C. § 1956 (laundering the proceeds of smuggling and conducting financial transactions to promote smuggling); 18 U.S.C. § 371 (conspiracy to commit the foregoing offenses), collectively, the "Subject Offenses" by Eugene Lantsman and his son, Leonid Lantsman.

5. The SUBJECT DEVICES from the New York Premises described in ¶ 3a and Attachment A were located, identified and seized pursuant to two warrants issued on



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

November 14, 2019, and November 20, 2019, under case numbers 19-M-1074 and 19-M-1101 respectively, by the Honorable James Orenstein, United States Magistrate Judge, Eastern District of New York.

6. The SUBJECT DEVICES from the Virginia Premises described in ¶ 3b and Attachment A were located, identified and seized pursuant to a search warrant issued on November 18, 2019, under case number 1:19-sw-1498 by the Honorable Michael Nachmanoff, United States Magistrate Judge, Eastern District of Virginia.

7. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

## DEFINITIONS

The following definitions apply to this Affidavit:

8. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

9. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, thumb drives, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

10. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

11. "Internet Service Providers (ISPs)," as used herein, are commercial organizations that are in business to provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers.

12. "Internet Protocol address" or "IP address" refers to a unique numbers used by a computer to access the Internet. An IP address often looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must be assigned an IP address so that the Internet traffic sent from, and directed to, that computer may be properly directed from its source to its destination. Most ISPs control the range of IP addresses. Some computers have a static – that is long term – IP address, while other computers have a dynamic – that is, frequently changed – IP address.

13. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. "Records," "documents," and "materials," as used herein, include all information and data recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

15. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

16. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, hard drives, RAM, thumb drives, flash memory, floppy disks, CD-ROMs, and other magnetic or optical media.

## SUMMARY OF PROBABLE CAUSE

As detailed infra, the FWS is investigating Eugene Lantsman and his son, Leonid Lantsman, for illegal trafficking in products and merchandise such as weapons, shields and flasks, made, in whole or in part, from wildlife. Based on my training and experience



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and the facts as set forth in this Affidavit, there is probable cause to believe that the contents of the SUBJECT DEVICES described in ¶ 3 supra and Attachment A, constitute evidence, fruits and instrumentalities of violations of federal criminal laws by Eugene and Leonid Lantsman including: 16 U.S.C. § 554 (smuggling goods out of the United States); 16 U.S.C. § 1538 (importing, exporting, taking, possessing, selling, delivering, receiving and offering for sale in interstate or foreign commerce endangered or threatened species of wildlife); 16 U.S.C. § 3372(a) (importing, exporting, transporting, selling, receiving, acquiring and purchasing in interstate or foreign commerce any fish or wildlife taken, possessed, transported, or sold in violation of any law or regulation of the United States or an individual State, or any foreign law); 16 U.S.C. § 3372(d) (making or submitting any false record or label for, or any false identification of, any wildlife which has been, or is intended to be, transported in interstate commerce or foreign commerce); 18 U.S.C. § 1956 (laundering the proceeds of smuggling and conducting financial transactions to promote smuggling); 18 U.S.C. § 371 (conspiracy to commit the foregoing offenses), collectively, (the "Subject Offenses").

**Federal Laws Relating to the Investigation**

17. The FWS enforces several laws and regulations relating to trafficking in wildlife including the ESA, 16 U.S.C Sections 1538 et seq.; the Convention on International Trade in Endangered Species of Wild Fauna and Flora ("CITES"), the Lacey Act Amendments of 1981, 16 U.S.C. Sections 3371 et seq.; and 18 U.S.C. Section 554.

18. CITES is an international treaty that provides protection to fish, wildlife and plants that may become imperiled due to the demands of international markets. CITES has been signed by more than 180 countries around the world. The United States has implemented CITES as part of the ESA and the regulations promulgated thereunder. See 16 U.S.C. § 1538(c)(l) (providing that "[i]t is unlawful for any person subject to the jurisdiction of the United States to engage in any trade in any specimens contrary to the



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

provisions of the Convention, or to possess any specimens traded contrary to the provisions of Convention..."); See also 50 C.F.R. Parts 14 and 23.

19. "Fish or wildlife" are defined, in pertinent part, as "any wild animal, whether alive or dead . . . and including any part [or] product . . . thereof." 50 C.F.R. § 10.12.

20. Based on my training and experience I know that species protected under CITES are listed in a series of appendices (Appendices I, II and III). Appendix I includes species threatened with extinction and provides the greatest level of protection. International trade in Appendix I species for primarily commercial purposes is essentially prohibited. Appendix II includes species that, although not currently threatened with extinction, may become so without trade controls. Under Appendix I of CITES and federal regulation, a CITES-protected species may be exported from the United States to a foreign country only if, prior to exportation, the exporter possesses a valid CITES export or re-export permit issued by United States and a valid CITES import permit issued by the foreign country. Under Appendix II of CITES and federal regulation, a species may be exported from the United States to a foreign country only if, prior to exportation, the exporter possesses a valid CITES export or re-export permit from the United States. 50 CFR § 23.20.

21. Under Federal regulations, wildlife may not be exported from the United States for commercial purposes without filing a completed Declaration for Importation/Exportation (Form 3-177), certified by the exporter or his agent, with the FWS. 50 CFR § 14.63. To obtain clearance, the exporter must make available all shipping documents (including bills of lading, waybills, and packing lists or invoices). 50 CFR § 14.52.

22. Congress has passed statutes that criminalize the importation, export or possession of wildlife trafficked in violation of federal laws and regulations, including CITES. Among them, 18 U.S.C. § 554 makes it a felony for a person to fraudulently or knowingly export or send from the United States, any merchandise, article or object



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contrary to law, or receives, conceals, buys, sells or in any manner facilitates the transportation, concealment or sale of such merchandise prior to exportation, knowing the same to have been exported from the United States contrary to law.

**The Investigation**

Initial Package Interception

23. On or about September 27, 2018, a package was intercepted by the United States Customs and Border Protection ("CBP") at the United States Postal Service International Mail Facility ("USPS IMF") at John F. Kennedy International Airport ("JFK") in Queens, New York (the "Subject Package"). The Subject Package listed the sender's name as "Eugene Lantsman," provided 950 72nd Street, Apt. # 2A, Brooklyn, New York 11228 (i.e., the New York Premises) as the sender's address and was addressed to be sent to Hong Kong, China. The Subject Package was declared on a Customs form included in postal airway bill to contain "Antique Decorative Metalwork, Circa 1900, Origin China, Iron Brass" valued at $2,400. The tracking number assigned to the Subject Package was EZ117720415US.

24. A CBP officer opened and inspected the contents of the Subject Package. The Subject Package contained a sword with a handle that appeared to be composed of, or made from, wildlife. The CBP officer referred the package to the FWS.

25. On or about September 27, 2018, a FWS Inspector examined the Subject Package and identified the sword handle to be composed of what appeared to be sea turtle shell. There was no FWS Declaration Form 3-177 for this wildlife product attached to or included in the package, nor was one filed. The sword was subsequently seized by the FWS on November 27, 2018.

26. A Senior Forensic Scientist at the FWS National Fish and Wildlife Forensics Laboratory who received training in the identification of sea turtle parts, identified the sword handle to be composed of either Green Sea Turtle (*Chelonia mydas*) or Hawksbill Sea Turtle (*Eretmochelys imbricata*), both of which are listed as endangered under the ESA and listed under CITES Appendix I.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Identification of Arms and Antiques Inc.

27. An internet query for "Eugene Lantsman" returned results indicating that he was the "Chief Executive Officer" of "Arms and Antiques Inc."

28. An internet query for Arms and Antiques Inc., resulted in the discovery of WWW.ARMSANDANTIQUES.COM (the "Website").

29. A query of the New York State Department of State revealed that Arms and Antiques Inc., was registered as a "domestic business corporation" in Kings County, New York, on March 4, 2011. Eugene Lantsman is listed as the Chief Executive Officer and provides the New York Premises as the address of the business.

Interview of Eugene Lantsman

30. On February 21, 2019, a FWS Wildlife Inspector and I interviewed Eugene Lantsman.

31. Eugene Lantsman initially stated that Arms and Antiques Inc. was "not a business," but a hobby. He stated that he registered Arms and Antiques Inc. once he began selling items from his collection and annual sales exceeded $10,000.

32. Eugene Lantsman stated that he sells items "two, three times a year" and that sales are conducted at tradeshows or via the Website.

33. Eugene Lantsman stated that the Website is hosted by GoDaddy.com, LLC.

34. Eugene Lantsman stated that approximately "2%" of Arms and Antiques Inc.'s transactions involve importing and exporting shipments and that Arms and Antiques Inc. has shipped approximately "once in two years or three years" internationally.

35. Eugene Lantsman stated that prospective buyers contact him via the Website and messages are sent to "INFO@ARMSANDANTIQUES.COM" (the "Business Email"). Both Eugene Lantsman and his adult son, Leonid Lantsman, respond to email inquiries.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

36. Eugene Lantsman stated that both his home in Brooklyn, New York, and his son's home in Alexandria, Virginia, are used for the Arms and Antiques Inc. operations, including inventory.

37. Eugene Lantsman stated that Arms and Antiques Inc. receives payments for sales via cash or checks at tradeshows, and via PayPal or wire transfer for international transactions.

38. Eugene Lantsman stated that he purchased the sword with the turtle handle that was seized by the FWS (discussed supra at ¶¶ 24-26) at a flea market in Brimfield, Massachusetts, during the summer of 2018, for approximately $500-600. He then transported the sword to the New York Premises.

39. Eugene Lantsman stated that the buyer of the sword initially contacted him via the Website and they communicated via the Business Email regarding the price and shipping of the sword.

40. Eugene Lantsman stated that he sold the sword for $18,000 and that it was being shipped to Hong Kong, China.

41. Eugene Lantsman claimed that he did not suspect this sword was composed of sea turtle shell, though he admitted he was knowledgeable of the characteristics of sea turtle shell. Eugene Lantsman further claimed that he was not aware that items he previously sold or had in his collection contained wildlife, including "crocodile leather, stingray leather, cow, buffalo horn, walrus ivory, elephant ivory, possible tortoise shell, deer, stag horn, coral."

Review of the Website for Wildlife Products

42. From February 2019 through October 2019, other law enforcement agents and I reviewed the publicly viewable Website. From that review, FWS identified approximately 87 items that had been sold that were described by the Website as containing, or which, based on included photographs, appeared to contain federally regulated wildlife. A partial list of items sold via the Website which contained wildlife items regulated under ESA and CITES includes:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. An "Antique Japanese Muromachi Period 16th c. Tanto Dagger with NBTHK Papers for Osafune Kiyomitsu" described as containing, and including a photograph which appeared to contain, "shark skin" and what appeared to be elephant ivory.

b. A "Magnificent 18th C. Shield from the Udaipur Maharana Sangram Singh II of Mewar" described as containing "rhinocerous [*sic*] hide."

c. A "Rare 19th C. Scottish or German Whale Tooth Powder Flask" described as containing, and including a photograph which appeared to contain, a "whale tooth."

d. An "Ethiopian Abyssinian Shotel Sword" which included a photograph which appeared to contain rhinoceros horn.

Review of Arms and Antiques Inc. Import/Export History

43. On April 19, 2019, I reviewed the import/export history for the New York Premises and Virginia Premises addresses associated with Arms and Antiques Inc.

44. From October 2012, to February 2019, Eugene and Leonid Lantsman exported approximately 61 packages from the United States, with approximately 52 of those shipments declared to contain antiques or metal. Shipment destination countries included, in part, Qatar, France, Australia, China and Russia.

45. From August 2010 to March 2019, Eugene and Leonid Lantsman imported approximately 38 packages into the United States, with approximately 23 of those shipments declared to contain antiques.

46. A query of the FWS Law Enforcement Management Information System ("LEMIS") revealed that Arms and Antiques Inc. applied for and was issued a FWS import/export license in December 2014, which expired in November 2015. The application documents associated with this license stated that Leonid Lantsman was the president of Arms and Antiques Inc. The applicant also signed the section of the application which certified that they "have read and am familiar with the regulations



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contained in Title 50, Part 13 of the Code of Federal Regulations and the other applicable parts in subchapter B of Chapter 1 of Title 50."[1]

47. Arms and Antiques Inc., applied for and was issued a renewal FWS import/export license in November 2015, which expired in October 2016. There has been no application for renewal by Arms and Antiques Inc. since October 2016.

48. A query of the FWS LEMIS revealed that Arms and Antiques Inc. declared one export of a weapon containing walrus ivory to Austria on December 15, 2015. Leonid Lantsman applied for the CITES permit which accompanied this shipment to Austria. In the application documents, Leonid Lantsman highlighted his identification credentials by stating the following, "I specialize in antique arms and armor focusing on oriental and eastern items from China, Korea, Japan, India and the Caucasus region. I have catalogued artifacts in the Smithsonian Museum Anthropology Archives. Specifically, I was responsible for identifying and cataloguing oriental arms and armor items in the Smithsonian Anthropology archives in Suitland, Maryland."

Review of Arms and Antiques Inc. PayPal Records

49. On April 19, 2019, I reviewed records for two PayPal Holdings, Inc. accounts registered to Arms and Antiques Inc., which were opened in August 2000, and March 2011. As of April 2, 2019, these accounts had received $1,329,384.48 and had sent $466,915.46. Both of the PayPal accounts included the New York Premises as a registered address for a "Home or Work" address.

50. These PayPal accounts identified approximately 86 international transactions associated with Arms and Antiques Inc.

Review of Business Email Communications

51. On April 30, 2019, the Honorable Ramon E. Reyes, Jr., United States Magistrate Judge for the Eastern District of New York, issued a search warrant for information associated with the Business Email (i.e., INFO@ARMSANDANTIQUES.

[1] Title 50, Part 13 of the Code of Federal Regulations outlines the FWS "General Permit Procedures," while the remaining parts outline various FWS regulations, including import/export declaration and CITES requirements.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

COM) in the possession of Google Inc. From May 2019 through October 2019, I reviewed documents associated with the Business Email, including communications sent from and received by the Business Email. This review was inclusive of communications sent and received from January 1, 2015, to February 21, 2019. Both Eugene and Leonid Lantsman used the Business Email to communicate with clients and each other.

52. My review of email communications revealed multiple conversations highlighting Eugene and Leonid Lantsman's knowledge of wildlife identification, including ivory, sea turtle shell and rhinoceros horn, many of which occurred prior to September 27, 2018.

53. My review of email communications revealed multiple conversations, many occurring prior to September 27, 2018, highlighting Eugene and Leonid Lantsman's knowledge of federal wildlife and customs regulations - specifically, the prohibition of shipping items containing wildlife outside of the United States without declaration to FWS and CITES permits.

54. My review of email communications revealed multiple instances of Eugene and Leonid Lantsman selling, offering to ship and shipping wildlife products in violation of federal and state regulations, examples of which include:

a. In May 2015, Leonid Lantsman sold and shipped one sword, described as having a shark skin scabbard, to China via USPS tracking number EZ061116705US. The sword was sold for $4,675 including shipping.

b. In December 2016, Leonid Lantsman sold and shipped one sword, described as having a stingray skin handle, to Hong Kong via FedEx tracking number 777983890516. The sword was sold for $18,150 including shipping.

c. In January 2017, Leonid Lantsman sold and paid for the shipment of one sword, described as having an ivory handle, to Canada via FedEx tracking number 778183785276. The sword was sold for $5,400.

d. In August 2017, Eugene Lantsman sold and shipped one sword, described as including walrus ivory, to Hong Kong via USPS



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

tracking number EZ049392302US. The sword was sold for approximately $2,900.

e. In September 2018, Eugene Lantsman sold and Leonid Lantsman shipped one sword with sea turtle shell handle to Hong Kong via USPS tracking number EZ117720415US. The sword was sold for $18,000. This was the sword that was seized by the FWS as set forth in ¶¶ 24-26 supra.

f. In February 2019, Eugene Lantsman offered to ship one sword, described as having a rhinoceros handle, to Hong Kong. This sword was being offered as a replacement to the buyer of the sword that was seized by the FWS as set forth in ¶¶ 24-26 supra.

55. My review of email communications observed multiple communications that confirmed that Arms and Antiques Inc.'s inventory is stored in the New York and Virginia.[2] Notable communications include:

a. On April 9, On April 9, 2015, while discussing potential items for sale, Leonid Lantsman stated, "My collection is in DC. If you'll be down here I'd be happy to host you to view the collection and then lunch or dinner if it would be on a weekend."

b. On June 20, 2015, while discussing the sale of a "Gorgeous 19th C. Chinese jade Screen inlaid with Hardstones Ex.," Leonid Lantsman stated, "Ok great. I'll put it on hold until payment and can have it shipped from my NY location."

c. On October 13, 2017, while discussing potential items for sale, Leonid Lantsman stated, "I ended up purchasing the entire collection. You can view at my fathers [*sic*] house if you're interested."

d. On November 12, 2017, while discussing potential items for sale, Leonid Lantsman stated, "Yes we have several new fine swords.

[2] Leonid Lantsman lives in Alexandria, Virginia, which is bounded to the East by the Potomac River. Alexandria, Virginia is south of Washington, D.C., which is bounded to the West by the Potomac River. The U.S. Census Bureau recognizes the "Washington-Arlington-Alexandria DC-VA-MD-WV Metropolitan Statistical Area," which is sometimes referred to as "the D.C. Area."



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

They're at my fathers [*sic*] house. I'd recommend you set up a time to visit him in Brooklyn and you can view everything in person."

e. On January 18, 2019, while discussing potential items for sale, Leonid Lantsman stated, "I'm based in Washington DC and New York."

Search of the New York Premises

56. On November 14, 2019, the Honorable James Orenstein, United States Magistrate Judge for the Eastern District of New York issued a search warrant for the New York Premises, including an associated storage unit at the same location, and any locked and closed items contained therein.[3]

57. On November 20, 2019, the United States executed the November 14, 2019 Search Warrant for the New York Premises.

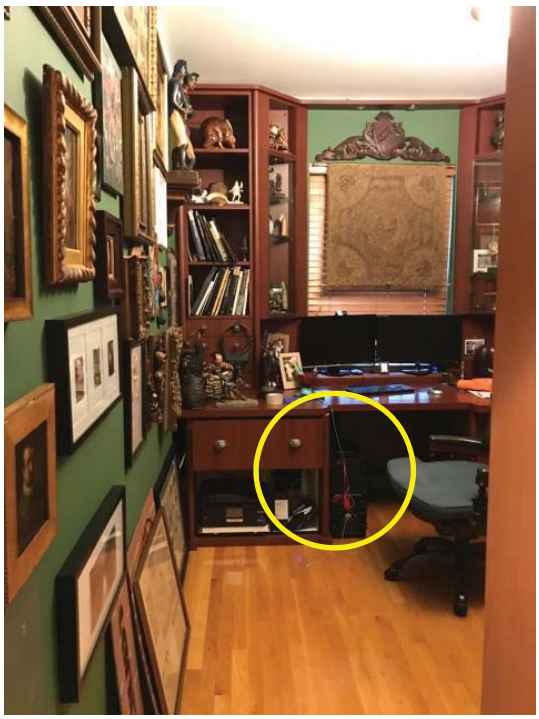
58. During the execution of the Search Warrant, Marina Lantsman, the wife of Eugene Lantsman returned home. Marina Lantsman told law enforcement agents that she did not work for Arms and Antiques Inc. In sum and substance, she advised law enforcement agents that there was a computer in the home office of her husband, Eugene Lantsman. In sum and substance, Marina Lantsman stated that her husband used the computer and that she did not use it, as she only used her cellphone.

59. During the search of the New York Premises, law enforcement agents located a home office which contained the computer and numerous antique weapons, antique items and non-fiction books concerning antique weapons, armor and metals. Many of the weapons seized contained parts made from wildlife. Photographs of Eugene Lantsman's home office showing the location of the computer are included below:

[3] The Court denied the government's application in part. Specifically, the Court denied the portion of the application seeking permission to seize computers or storage media in the New York Premises because *inter alia* the affidavit in support of the application for the warrant did "not include any allegation that the suspect keeps any [] computers or storage media in the New York Premises." Nonetheless, the Court further found that "the government may conduct a search of the premises for paper records and other physical evidence or instrumentalities of the offenses under investigation . . . and then, if it discovers electronic devices, return to the court seeking a warrant to search those devices."



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



60. The computer appeared to be a home-built or specially constructed computer, as opposed to an already assembled computer available at retail, because it uses a separately purchased housing unit that can contain separately purchased computer components. The component parts of the computer could not be identified without opening the housing unit.

61. Also during the execution of the Search Warrant, law enforcement agents located a hard drive in a closet in the living room of the New York Premises. The hard drive appears to be one that could be a component of the computer or attached to the computer as external storage.

62. Accordingly, on November 20, 2019, the United States made an application for a warrant to seize the computer and hard drive located at the New York Premises. The Honorable James Orenstein, United States Magistrate Judge, granted the application and issued a warrant permitting the seizure of the computer and hard drive (the "November 20, 2019 Warrant").

63. Pursuant to the November 20, 2019 Warrant, law enforcement agents seized the computer and hard drive. Thereafter, the computer and hard drive were



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

shipped to FWS's Digital Evidence Recovery and Technical Support Unit located at 17930 International Blvd., SeaTac, Washington.

Search of the Virginia Premises

64. On November 18, 2019, the Honorable Michael Nachmanoff, issued a search warrant for the Virginia Premises, which are also the residential premises of Leonid Lantsman. The November 18, 2019 warrant permitted the seizing of certain devices from the Virginia Premises.[4]

65. On November 20, 2019, during the search of the Virginia Premises, law enforcement officers located the SUBJECT DEVICES listed in ¶ 3b above and Attachment A on the premises and established probable cause to believe that they would contain records relating to, and instrumentalities of, violations of 16 U.S.C. §§ 1538, 3372(a)(2)(A) and 3372(d), and 18 U.S.C §§ 371 and 554, those violations including acts by Eugene Lantsman, Leonid Lantsman and Arms and Antiques Inc. The SUBJECT DEVICES from the Virginia Premises were seized by the FWS and forensic mirror images were taken from them. After the SUBJECT DEVICES listed in ¶ 3b were forensically mirror imaged, the original devices were left at the Virginia Premises. The forensic mirror images were subsequently shipped to the agency's Digital Evidence Recovery and Technical Support Unit located at 17930 International Blvd., SeaTac, Washington.

//

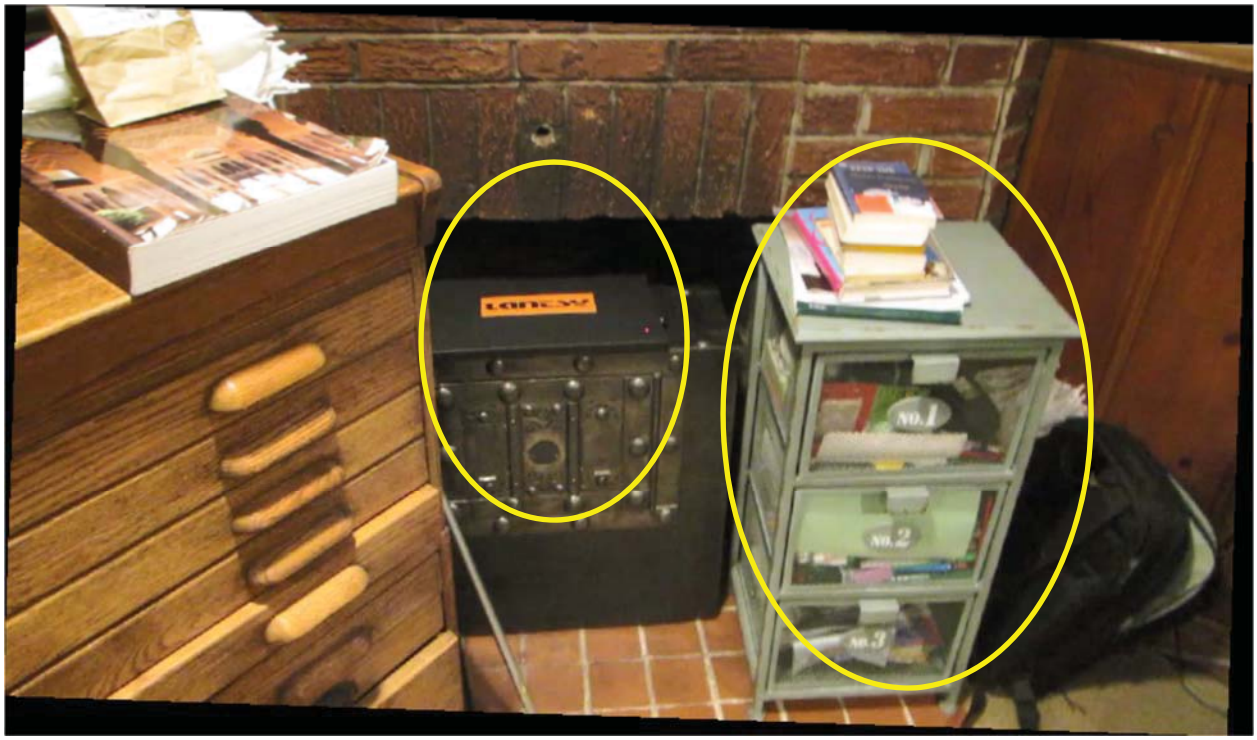
//

[4]Therefore, while the FWS might already have all necessary authority to examine the forensic mirror images from SUBJECT DEVICES located at Virginia Premises, I seek this additional authority out of an abundance of caution to be certain that an examination of these images will comply with the Fourth Amendment and other applicable laws.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

66. Photographs of Leonid Lantsman's basement showing the location of the SUBJECT DEVICES that were imaged at the Virginia Premises are included below:





UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

67. Senior Special Agent (SSA) Brian Russell served as the lead digital evidence recovery agent for the search of the Virginia Premises on November 20, 2019. During the search, the Lenovo ThinkPad T560 laptop was identified by a member of the team. While documenting the status of the laptop, SSA Russell observed that it was in a "powered on" state indicated by a light on the top of the closed lid. He further observed the laptop was connected to a wired keyboard and monitor and a wireless mouse. The external monitor was in a "powered off" state. SSA Russell powered on the monitor using a remote control found on the desk, and observed a web browser running with five open tabs. As part of the documentation process during data acquisition, it was necessary to look at running programs and other items on the computer in an effort to determine if encryption was present that may require the data to be acquired without powering down the computer system. Three of the five tabs displayed content that was related to a website called "the saleroom". The other two tabs were related to Gmail. The web page title is listed on the tabs. The email addresses listed on the two Gmail tabs were leonid.lantsman@gmail.com and info@armsandantiques.com.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

68. As shown above in ¶ 66 supra, all of the SUBJECT DEVICES described in ¶ 3b supra were found in the basement of the Virginia Premises, and more particularly, in the vicinity of the laptop, keyboard and monitor described in ¶ 67 supra. Based on my experience and search of the Virginia Premises, I believe the basement was used as a home office for the operations of Arms and Antiques Inc. As the WEBSITE contained digital photos of items purchased, marketed, sold and shipped by the Lantsmans, I believe there is probable cause to believe that the SUBJECT DEVICES described in ¶ 3b supra contain electronic evidence of items in violation of the Subject Offenses.

69. Following the seizure of the forensic mirror images of SUBJECT DEVICES, FWS shipped the forensic mirror images to FWS's Digital Evidence Recovery and Technical Support Unit at 17930 International Blvd. in SeaTac, Washington, where they remain today. The analysis and review contemplated by this search warrant application would take place at that location.

70. In my training and experience, I know that the SUBJECT DEVICES from the New York Premises and forensic mirror images of SUBJECT DEVICES from the Virginia Premises have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of the FWS.

71. Based on my training and experience, the results of the criminal investigation to date and the information relayed to me by other law enforcement officers with experience in investigating wildlife trafficking crimes and related offenses, I believe that evidence, fruits and instrumentalities of the subject offenses listed in this Affidavit is likely to be found on the SUBJECT DEVICES and forensic mirror images of the SUBJECT DEVICES.

72. Based on my training and experience, I know that wildlife traffickers commonly use electronic means, including computers, to coordinate the purchase, shipment, and payment for internationally smuggled wildlife.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

73. Furthermore, based on my training and experience, I know that the continuing viability of criminal operations dealing in the illegal smuggling of wildlife is dependent upon the storage of such information, either electronically, manually written, or both. Additionally, customer lists, customer contact information, shipping records and bank records are essential. Persons engaged in these kinds of activities tend to keep this information readily and conveniently accessible electronically through computers, manually written, or both.

## TECHNICAL BACKGROUND

74. As part of my training and experience, I have become familiar with the Internet, a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

75. Based on my training and experience, and that of computer forensic agents that I work and collaborate with, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another. As a result, I believe that electronic evidence may have been stored on the SUBJECT DEVICES specified in this Affidavit and in Attachment A.

76. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases, the items set forth in Attachment B may take the form of files, documents, and other data



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data – including in some cases data generated automatically by the devices themselves.

77. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe there is probable cause to believe that the items and records set forth in Attachment B will be stored in the SUBJECT DEVICES set forth in this Affidavit and in Attachment A, for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices – in particular, a computer's internal hard drive – contain electronic evidence of how a digital device has been used, what is has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information – and, the use of such special software may itself result in ESI that is relevant to the



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

criminal investigation. FWS agents in this case have consulted on computer forensic matters with law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

## SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

78. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly controlled environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since ESI is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code embedded in the system such as a "booby trap"), a controlled environment is often essential to ensure its complete and accurate analysis.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Volume of Evidence: The volume of data stored on many digital devices is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally, this data may be stored in a variety of formats or may be encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer).

c. Search Techniques: Searching the ESI for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

79. In this particular case, the search techniques that will be applied include:

a. Filename review.

b. Directory structure review.

c. Hash analysis.

d. File signature analysis.

e. Keyword searches.

f. Document review by file type.

g. Image file review.

h. Video file review.

i. Review of messaging service data.

j. Email searches with/without attachments.

k. Internet history review.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

l. Timeline analysis.

m. Installed software/programs review.

n. Searches for possible encryption/passwords.

o. Location data review.

p. Data carving.

q. Deleted file review.

r. Recycler/Recycle Bin analysis.

s. Windows registry analysis.

t. Windows operating system analysis.

u. Other computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine-whether it is evidence described by the warrant.

80. The search techniques may not all be required or used in a particular order for the identification of digital devices containing items, information or data set forth in Attachment B. However, these search techniques will be used systematically in an effort to protect against viewing unrelated personal documents and files. Use of these tools will facilitate the quick identification of items, information and data authorized to be seized pursuant to Attachment B, and will also assist in the early exclusion of digital devices, and/or files which do not fall within the scope of items, information and data authorized to be seized pursuant to Attachment B.

## COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

81. Based on my knowledge, training, and experience, I know that digital devices and electronic storage store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. In my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the device.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

82. There is probable cause to believe that things that were once stored on the SUBJECT DEVICES may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

83. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

84. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

85. Manner of execution. Because this warrant seeks only permission to examine SUBJECT DEVICES or forensic images already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

## SEARCH TECHNIQUES

86. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will authorize:

a. Imaging or otherwise copying all data contained on the SUBJECT DEVICES seized from the New York Premises.

b. A review and examination of the images or copies of all the SUBJECT DEVICES seized from both the New York Premises and Virginia Premises (and identified in ¶ 3 supra) consistent with the requested warrant.

87. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of the SUBJECT DEVICES and images or copies therefrom pursuant to this warrant as follows:

### Securing the Data



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image or copy, if possible and appropriate, of the SUBJECT DEVICES from the New York Premises. Forensic images of the SUBJECT DEVICES from the Virginia Premises have already been secured.

b. Law enforcement will only create an image of data physically present on or within the SUBJECT DEVICES from the New York Premises. Creating an image of the SUBJECT DEVICES will not result in access to any data physically located elsewhere. However, SUBJECT DEVICES that have previously connected to devices at other locations may contain data from those other locations.

**Searching the Forensic Images**

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.

b. These methodologies, techniques, and protocols may include the use of a "hash value" library to exclude normal operating system files that do not need to be further searched. Agents may utilize hash values to exclude certain known files, such as the operating system and other routine software, from the search results. However, if the evidence I am seeking does not have particular known hash values, agents will not be able to use any type of hash value library to locate the items in Attachment B.

//

//



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## CONCLUSION

88. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Curtis Knights

CURTIS KNIGHTS
Special Agent
United States Fish and Wildlife Service

Subscribed and sworn to through the transmission of this Application by reliable electronic means, pursuant to Federal Rule of Criminal Procedure 41(d)(3) and 4.1 on July 31, 2020

UNITED STATES MAGISTRATE JUDGE



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## ATTACHMENT A

The property to be searched includes:

a. SUBJECT DEVICES located, identified at, and subsequently seized from the residential premises located at 950 72nd Street, Apt. #2A, Brooklyn, New York 11228 ("the New York Premises"):

| Item Description | FWS Evidence Number |
|---|---|
| 1. Computer housed in a "Cooler Master" brand housing tower and bearing the bar code RC912KKN11131500811 | ST# 075402 Item 1 |
| 2. 1 Terabyte Western Digital WD10EALX Hard Drive bearing the serial number WCATR9321079 | ST# 075402 Item 2 |

b. Forensic mirror images of SUBJECT DEVICES located, identified at, and seized from the residential premises located at 704 Devon Place, Alexandria, VA 22314 (the Virginia Premises):

| Item Description (from which forensic mirror images were taken) | FWS Evidence Number |
|---|---|
| 1. Lenovo ThinkPad T560 laptop computer bearing S/N R9-0MEHEJ containing SanDisk SSD hard drive bearing S/N 164813800597 | ST# 064100 Item 1A |
| 2. 8GB San Disk SD card bearing S/N B11105716254G | ST# 064100 Item 2A |
| 3. 2GB Vector Media USB flash drive | ST# 064100 Item 3A |
| 4. 32 MB Gateway USB flash drive | ST# 064100 Item 4A |
| 5. 2GB SanDisk Cruzer USB flash drive bearing S/N 07741302A3A1446C | ST# 064100 Item 5A |
| 6. 8GB Kingston USB flash drive bearing S/N 201006010301 | ST# 064100 Item 6A |
| 7. 256 MB USB flash drive bearing S/N 1000026150007 | ST# 064100 Item 7A |
| 8. 16GB PNY USB flash drive bearing S/N AA0000000034 | ST# 064100 Item 8A |
| 9. 4GB USB flash drive | ST# 064100 Item 9A |



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

| | |
|---|---|
| 10. 2GB SanDisk SD card bearing S/N BE0808713287G | ST# 064100 Item 10A |
| 11. 2GB Exelis USB flash drive bearing S/N 9E4F9DAA | ST# 064100 Item 11A |
| 12. 1GB unknown model USB flash drive | ST# 064100 Item 12A |
| 13. 16GB Patriot USB flash drive with S/N 070C4421A506AC63 | ST# 064100 Item 13A |
| 14. 64GB SanDisk Cruzer USB flash drive with S/N 4C530001310607113470 | ST# 064100 Item 18A |

The SUBJECT DEVICES and the forensic images of SUBJECT DEVICES are currently being stored at the FWS OLE Digital Evidence Recovery and Technical Support Unit, SeaTac, Washington. In my training and experience, I know that the SUBJECT DEVICES and forensic images of SUBJECT DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of the FWS.

This warrant authorizes the forensic examination of the SUBJECT DEVICES and forensic images of SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## ATTACHMENT B

1. The following records on the SUBJECT DEVICES and forensic images of SUBJECT DEVICES described in Attachment A that relate to violations of federal criminal laws, including: 16 U.S.C. § 554 (smuggling goods out of the United States); 16 U.S.C. § 1538 (importing, exporting, taking, possessing, selling, delivering, receiving and offering for sale in interstate or foreign commerce endangered or threatened species of wildlife); 16 U.S.C. § 3372 (importing, exporting, transporting, selling, receiving, acquiring and purchasing in interstate or foreign commerce any fish or wildlife taken, possessed, transported, or sold in violation of any law or regulation of the United States or an individual State, or in violation of any foreign law); 16 U.S.C. § 3372 (making or submitting any false record or label for, or any false identification of, any wildlife which has been, or is intended to be, transported in interstate commerce or foreign commerce); 18 U.S.C. § 371 (conspiracy to commit the foregoing offenses), collectively, (the "Subject Offenses") by Eugene Lantsman and his son, Leonid Lantsman since 2014:

a. Evidence that items purchased, possessed, advertised for sale, sold, and/or shipped contained, or were made from, wildlife;

b. Evidence that Eugene Lantsman and/or Leonid Lantsman knew, or were on notice of the possibility, that items they purchased, possessed, advertised for sale, sold, and/or shipped contained, or were made from, wildlife;

c. Evidence of Eugene Lantsman or Leonid Lantsman's knowledge of the Lacey Act,the Endangered Species Act ("ESA"), and/or of laws, regulations, requirements and prohibitions concerning the importing, exporting, transporting, selling, receiving, acquiring and purchasing in interstate or foreign commerce of any fish or wildlife taken, possessed, transported, or sold in violation of any law or regulation of the United States or an individual State, or in violation of any foreign law;

d. Lists of customers and related identifying information;



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. Any information concerning the types, amounts, descriptions, identification number, and/or prices of items containing, or made from, wildlife; as well as dates, places, and/or amounts of specific transactions, possession or shipments;

f. Any information related to sources of items containing or made from wildlife (including names, addresses, phone numbers, or any other identifying information);

g. Communications concerning items containing wildlife;

h. Any information concerning the regulation of the possession, trading, purchase, sale, importation, exportation and/or shipping of items containing wildlife;

i. Any information concerning the identification of whether items contain wildlife;

j. Any information concerning CITES permits, CITES permit applications, import/export licenses and/or applications for import/export licenses;

k. Any information documenting Eugene Lantsman or Leonid Lantsman's schedule or travel from January 1, 2014, to November 20, 2019;

l. All bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the items, information, and/or data described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

As used above, the term "wildlife" means "any wild animal, whether alive or dead . . . and including any part [or] product . . . thereof." 50 C.F.R. § 10.12.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

As used above, the term "CITES" means the Convention on International Trade in Endangered Species of Wild Fauna and Flora. 50 C.F.R. Part 23.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970